

REMARKS/ARGUMENTS

Claims 1-27 are pending in the application. Reconsideration is requested in view of the above amendments and the following remarks.

1. The Drawing.

The Examiner has required that a drawing be submitted, asserting that the subject matter admits of illustration to facilitate an understanding of the invention. Applicant submits a proposed drawing herewith for consideration by the Examiner, along with an amendment to the Specification. Reconsideration and approval of the drawing is respectfully requested.

2. The 102(e) Rejection over Feigen should be withdrawn.

Claims 1-4, 6, 8, 11, 13-21, 23 and 25 stand rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Application 2002/0138544 ("Feigen"). This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection is hereby respectfully requested.

The Applicant's invention is not disclosed or suggested by the Feigen reference and should be patentable. The Examiner contends that Feigen discloses providing a hash code table of a client; providing a client state code of a client; and comparing said client state code to said hash code table (referring to Pars. 8 and 10). The Examiner further asserts that Feigen discloses a secure hash code table (par. 8), and that Feigen discloses at

least one compiled client hash value (pars. 8 and 10); and generating an alert mechanism when a deviation threshold is reached based on a deviation between said hash code table

values for said client and said client state code (citing par. 16 of Feigen). The Examiner also contends that Feigen (at pars. 8, 10 and 16) teaches reporting the results of the comparison and initiating a client status mechanism.

Applicant's present invention is not taught, suggested or disclosed by Feigen. Applicant, as recited in claim 1, and as amended to more particularly articulate this feature of the invention, recites:

providing a hash code table of a client said hash code table being provided for storing a plurality of files;

providing a client state code of a client;

comparing said client state code to said hash code table, and

generating an alert mechanism when a deviation threshold is reached

based on a deviation between said hash code table values for said client and said client state code.

The claimed hash code table of a client is a feature which distinguishes the Applicant's invention over Feigen. Claims 18 and 19 are also similarly amended to recite this feature. Support for the amendment is contained in the Applicant's Specification, see for example, pars. 16-21 of the published application. Applicant's invention by employing the recited features has the ability to consider a level of deviation, and determine whether

there is deviation by an unacceptable amount, and if so, then triggering alerting mechanisms.

The passages of the Feigen reference cited and relied on by the Examiner do not appear to teach, suggest or disclose the Applicant's claimed hash code table. The cited passages of Feigen relied on by the Examiner read as follows:

[0008] The present invention provides a secure hash algorithm coupled with a random seed value which may be employed by a network host to verify the integrity of software (e.g., applications, operating system, configuration file, or the like) associated with a plurality of remote network appliances served by the network host. The software integrity verification process of the present invention may be applied in the context of cable television set top boxes, paid programming television modules, cellular telephone networks, PC-based LAN/WAN networks or essentially any other wired or wireless network in which there is a need for the network host or service provider to monitor the configuration of the remote network appliances.

* * *

[0010] The secure software integrity verification technique of the present invention requires at least limited bidirectional communication between the host and the various network appliances connected to the host. In order for the host to confirm that a block of code resident in the client device has not been tampered with, the host performs a hash function on a copy of the code under inspection which is maintained by the host. The host then transmits the hash function to the remote device whereupon the remote device performs the same hash function on the "same" block of code resident in the remote device. The remote device then transmits the resulting hash value back to the host, whereupon the host compares the initial hash value obtained by the host to the hash value received from the remote device. If the two hash values match, the host concludes that the block of code resident in the remote device corresponds to the copy of that same block of code maintained by the host. If, on the other hand, the two hash values do not match, the hosts may conclude that the block of code resident in the remote device has been tampered with or otherwise corrupted.

Even if the Examiner were to consider Feigen to in the most obscure but broad sense to be in some way disclosing a table of one, that is not the Applicant's invention when fairly considered. Applicant's invention recites a hash code table for storing a plurality of files. That is different than what is recited in Feigen. Feigen merely discloses that if "the two hash values do not match, the hosts may conclude that the block of code resident in the remote device has been tampered with or otherwise corrupted." (Par. 10). Feigen's comparison is of two hash values, not a table of hash values, and not the table of hash values Applicant discloses and claims. Applicant's invention utilizes a hash code table to provide a baseline for the network and for systems on the network. (See Applicant's Specification par. 13 of the published application.) For these reasons, Feigen fails to teach, suggest or disclose the Applicant's presently claimed invention.

Moreover, when considered as a whole, Feigen actually teaches away from the applicant's invention in that Feigen, in Par. 11, discloses a table to be a look-up table, or a database. Thus, Feigen's own disclosure is a table of random seeds for random generation by the host and insertion into a block of data under inspection. A reading of Feigen thus provides contrary teachings to the claimed *hash code table of a client* (E.g., not a random seeds table) which Applicant discloses and claims as its present invention. Therefore, Feigen actually teaches away from the present invention, and does not disclose what the Applicant claims as its invention.

In addition, claim 25 should be patentable over Feigen for the above reasons, and for additional reasons. Claim 25 recites -- wherein said hash code table is operable for

one or more client platforms --. Feigen, in addition to its lack of disclosure of Applicant's claimed hash code table of a client, also does not appear to suggest or disclose a hash code table (which Feigen does not even have) operable for one or more client platforms. This feature, which is recited and claimed in Applicant's claim 25, is not disclosed or suggested by Feigen. For the above reasons, and these additional reasons, claim 25 should be patentable over Feigen.

2. Claims 5 and 26-27 Should Be Patentable Over Feigen and Crockett.

Claims 5 and 26-27 stand rejected under 35 U.S.C. 103(a) as being obvious in view of Feigen as applied to claim 3, in view of US Patent 5,619,644 ("Crockett"). This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection is hereby respectfully requested.

This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection is hereby respectfully requested. Each of claims 5 and 26-27 depends from a claim rejected under Feigen, and discussed above. For the same reasons as those set forth above in connection with Applicant's reasons why Feigen fails to teach or disclose the Applicant's claimed invention, the further combination of Crockett still does not suggest or disclose the invention.

3. Claim 7 Should Be Patentable Over Feigen and IEEE.

Claim 7 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Feigen, as applied to claim 3, and in view of IEEE. This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection is hereby respectfully requested.

For the same reasons set forth above, Applicant's invention should be patentable over Feigen, even when the Examiner attempts to combine the further reference of IEEE. Accordingly, reconsideration and a withdrawal of the rejection is hereby respectfully requested.

4. Claims 9 and 22 Should Be Patentable Over Feigen.

Claims 9 and 22 stand rejected under 35 U.S.C. 103(a) as being obvious in view of Feigen. This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection is hereby respectfully requested.

Each of claims 9 and 22 depends, respectively, from one of the claims rejected under Feigen. For the same reasons as those set forth above in connection with Applicant's reasons why Feigen fails to teach or disclose the Applicant's claimed invention, claims 9 and 22 should also be patentable.

5. Claim 10 Should Be Patentable Over Feigen and Adya.

Claim 10 stands rejected under 35 U.S.C. 103(a) as being obvious in view of Feigen. This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection is hereby respectfully requested.

Claim 10 depends from claim 1. For the same reasons as those set forth above in connection with Applicant's reasons why Feigen fails to teach or disclose the Applicant's claimed invention, claim 10 should also be patentable, even when the Examiner attempts to combine the further reference of Adya. Accordingly, reconsideration and a withdrawal of the rejection is hereby respectfully requested.

6. Claims 12 and 24 Should Be Patentable Over Feigen and Pascucci.

Claims 12 and 24 stand rejected under 35 U.S.C. 103(a) as being obvious in view of Feigen as applied to claim 1, and in view of Pascucci. This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection is hereby respectfully requested.

Each of claims 12 and 24 depends, respectively, from one of the claims rejected under Feigen. For the same reasons as those set forth above in connection with Applicant's reasons why Feigen fails to teach or disclose the Applicant's claimed invention, claims 12 and 24 should also be patentable, even when the Examiner attempts to combine the further reference of Pascucci. Accordingly, reconsideration and a withdrawal of the rejection is hereby respectfully requested.

7. Double Patenting Rejection.

Applicant notes the Examiner's provisional rejection of claims 1-3, 8-11, 13-23, as being provisionally rejected in view of Applicant's copending application no. 10/032,252, and of claims 4-7, 12, and 24 (in view of the same application, but with additional references cited). Applicant will submit a terminal disclaimer in the event the Examiner maintains this rejection, but submits that the references relied on by the Examiner, for the reasons stated herein, do not render obvious claims 4-7, 12, and 24, and requests reconsideration of the rejection.

For the reasons set forth above, Applicant's invention is not disclose or suggested by the art of record not relied on.

Application Serial No. 10/032,251
Response dated: August 17, 2006
Reply to final Office Action of March 15, 2006

E-2528

CONCLUSION

Applicant's invention is not taught, suggested or disclosed by the cited references relied on by the Examiner. Accordingly, Applicant's presently claimed invention should be patentable.

If necessary, an appropriate extension of time to respond is respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required to Patent Office Deposit Account No. 05-0208.

Respectfully submitted,
JOHN F. A. EARLEY III
FRANK J. BONINI, JR.
CHARLES L. RIDDLE
HARDING, EARLEY, FOLLMER & FRAILEY
Attorneys for Applicant

Frank J. Bonini, Jr.
Registration No. 35,452
P.O. Box 750
Valley Forge, PA 19482-0750
Telephone: (610) 935-2300

Date: 8/17/06

It is a further object of the present invention to provide methods, apparatus and articles of manufacture that secure, maintain, monitor and control computer networks, including systems in networks, across a variety of platforms.

SUMMARY OF THE INVENTION

The preferred embodiments comprise methods, apparatus, and articles of manufacture for securing, maintaining, monitoring and controlling systems and networks. In the preferred embodiments, one or more secure hash code table(s) of the systems on the networks is generated. The secure hash code table may be generated through any or all of a number of methods. The secure hash code table provides a baseline for the network and the systems on the network.

At intervals, a comparison cycle occurs. One or more systems on the networks transmit a client state code. The client state code is compared to the secure hash code table value. If the client state code does not deviate from the secure hash code table value, or, in some embodiments, if the deviation is within acceptable ranges, then no action will be taken. If, however, there is deviation by an unacceptable amount, various alerting mechanisms will be triggered.

In certain preferred embodiments, a system repair method may be utilized through use of automated alert mechanisms and auto repair functions.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiments comprise methods, apparatus, and articles of manufacture for securing, maintaining, monitoring and controlling systems and networks. In the preferred embodiments, one or more secure hash code table(s) of the systems on the networks is initially generated. A secure hash code table is comprised of secure client

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic diagram illustrating an example of steps used in connection with carrying out the invention.